U.S. Department of the Interior
Office of Inspector General

AUDIT REPORT

MAINFRAME COMPUTER POLICIES AND PROCEDURES, ADMINISTRATIVE SERVICE CENTER, BUREAU OF RECLAMATION

REPORT NO. 97-I-683
MARCH 1997

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

MAY - 5 1997

MEMORANDUM

TO: The Secretary

FROM: Wilma A. Lewis
Inspector General

SUBJECT SUMMARY: Final Audit Report for Your Information - "Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation" (No. 97-I-683)

Attached for your information is a copy of the subject final audit report. The objective of the audit was to evaluate the adequacy of the management and internal controls of the mainframe computer system and processing environment of the Bureau of Reclamation's Administrative Service Center. Specifically, the audit focused on management and internal controls over the following areas: computer center management and operations; telecommunications and local area network security; application systems access; mainframe computer system physical and logical security; and contingency planning, backup, and disaster recovery.

We identified 15 weaknesses in the areas reviewed and made 24 recommendations for improving management and internal controls at the Service Center.

Based on the Bureau's response, we considered 13 recommendations implemented and 10 recommendations resolved but not implemented and requested the Bureau to reconsider the remaining recommendation, which related to improving internal controls over access to the mainframe computer.

If you have any questions concerning this matter, please contact me at (202) 208-5745 or Mr. Robert J. Williams, Assistant Inspector General for Audits, at (202) 208-4252.

Attachment

GLOSSARY

Asynchronous Protocol. Refers to a set of conventions used to start and stop transmissions that occur without a regular or predictable time relationship to a specific event. Synchronous protocol refers to a set of conventions used for transmissions that occur regularly or predictably with respect to a specific event.

Customer Information Control System (CICS). This is an IBM software product that serves as a teleprocessing monitor for the MVS operating system on the Service Center's mainframe computers, which enables transactions entered at remote computer terminals to be processed concurrently and is designed to control execution of application programs in an interactive on-line environment.

Data Structure. How the data are physically laid out within a computer system (for example, the fields in a record).

Ethernet. A networking scheme that allows microcomputers to be connected to a network. It physically consists of cabling, which connects all the machines on a network.

Multiple Virtual Storage/Enterprise Systems Architecture (MVS/ESA). An operating system that runs on IBM mainframe computers and increases virtual memory capability to 16 terabytes (trillion bytes),

Resource Access Control Facility (RACF). An IBM-licensed product that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, and logging detected accesses to protected resources.

Time Sharing Option (TSO). A system software product that serves as the session manager on the mainframe computers whereby terminal users can submit jobs on-line. Time sharing allows a number of users to execute programs concurrently and to interact with the programs during execution.

Transmission Control Protocol/Internet Protocol. The system that networks use to communicate with each other by allowing traffic to be routed from one network to another. The Internet Protocol is a set of conventions used to pass packets (that is, a cluster of data) from one network to another.

A-IN-BOR-00

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

MAR 31 1997

AUDIT REPORT

Memorandum

To: Assistant Secretary for Water and Science

From: Robert J. Williams
Assistant Inspector General for Audits

Subject: Audit Report on Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation (No. 97-I-683)

INTRODUCTION

This report presents the results of our audit of mainframe computer policies and procedures at the Bureau of Reclamation's Administrative Service Center. The objective of the audit was to evaluate the adequacy of the management and internal controls of the Service Center's mainframe computer system and its processing environment. Specifically, the audit focused on management and internal controls over the following areas: computer center management and operations; telecommunications and local area network (LAN) security; application systems access; mainframe computer system physical and logical security; and contingency planning, backup, and disaster recovery.

BACKGROUND

The Bureau of Reclamation's Administrative Service Center in Denver, Colorado, provides: (1) consolidated payroll and personnel services for about 106,000 employees in the Department of the Interior and five other Federal agencies and (2) Government accounting, integrated budgeting, and reporting services through the Federal Financial System (FFS) to five Departmental and five other Federal agencies.

At the time of our review, payroll and personnel services were provided through the Payroll/Personnel System (PAY/PERS). However, the Service Center was developing a new personnel/payroll system, the Federal Personnel Payroll System (FPPS). The first phase of the new system, which has been implemented, is the SF-52 System (an SF-52 form is entitled "Request for Personnel Action"). The second phase, which consists of personnel actions and payroll processing, is scheduled for implementation beginning in September 1997. The Service Center was also to provide payroll and personnel services to an additional 65,000 Social Security Administration employees beginning in October 1997.

The Service Center's ADP Services Division is responsible for managing the computer center that provides the various services. To assist the Division in carrying out its functions, the Service Center has contracted Tri-Cor to provide staff to assist in operating and maintaining the computer systems software, communications, and LANs. The computer center provides data processing support for several sensitive systems,[1] including PAY/PERS, FFS, SF-52, and FPPS. To support these systems, the computer center operates an IBM mainframe computer that runs Multiple Virtual Storage (MVS) Extended Systems Architecture operating system to manage the processing work load. The access control security software installed on the mainframe computer is the Resource Access Control Facility (RACF), which controls user access not only to the application systems, such as the Customer Information Control System applications, but also to the Time Sharing Option (TSO) facility. The FFS contains application level security that controls the action a user may invoke. Other system software, such as other data base management software, telecommunications software, and specialized vendor software products, also resides on the mainframe computers. Network and local communications support for both asynchronous and synchronous protocols are provided, as well as LAN connectivity, through Ethernet and Transmission Control Protocol/Internet Protocol. (The specific computer system software and network communications cited are detailed in the Glossary.)

SCOPE OF AUDIT

To accomplish our objective, we interviewed Service Center and Tri-Cor personnel, reviewed systems documentation, observed and became familiar with computer center operations and data structures, analyzed system security, and observed a disaster recovery test. In addition, we reviewed the software maintenance procedures. Because our review was limited to evaluating the adequacy of internal controls at the Service Center, we did not test the effectiveness of the internal controls at the various bureaus and agencies serviced by the Service Center.

Our audit, which was conducted during June through October 1996, was made in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the Service Center's system of internal controls over its mainframe computer system that could adversely affect the data processing environment, The control weaknesses that we found are discussed in the Results of Audit section and in Appendix 1 of this report. If implemented, our recommendations should improve the management and internal controls in the areas cited.

[1] According to the National Institute of Standards and Technology, sensitive systems are defined as "systems that contain any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any reports related to the scope of this audit. However, in March 1994, the Office of Inspector General issued the report "Compliance With the Computer Security Act of 1987, Denver Administrative Service Center, Bureau of Reclamation" (No. 94-I-357). The report stated that the Service Center generally complied with requirements of the Computer Security Act of 1987 but that improvements were needed in the areas of security and operations. Since the Service Center was addressing all of the deficiencies identified, no recommendations were made. However, deficiencies in performing a risk analysis of the Service Center's LANs and in the separation of duties within RACF software still existed during our review. These issues are discussed in the Results of Audit section and in Appendix 1 of this report.

RESULTS OF AUDIT

The Bureau of Reclamation's Administrative Service Center has weaknesses in management and internal controls in five major areas: (1) computer center management and operations; (2) LAN protection; (3) FFS application; (4) computer mainframe system physical and logical security; and (5) contingency planning, backup, and disaster recovery. Office of Management and Budget Circular A-130, "Management of Federal Information Systems," and the National Institute of Standards and Technology Federal Information Processing Standards Publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of 'executive branch agencies. Additionally, the Congress enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls is adequate. However, the Service Center has not complied with these criteria in that it did not document formal policies, standards, and procedures; follow proper practices and processes; segregate duties; comply with key software vendor guidelines for MVS integrity; and develop a formal, up-to-date, comprehensive data security program. These weaknesses increase the risk of unauthorized access and modifications to and disclosure of client-sensitive data supported by the Service Center's mainframe computer; theft or destruction of hardware, software, and sensitive information; and the loss of critical systems and functions in the event of a disaster.

Overall, we identified 15 weaknesses and made 24 recommendations for improving management and internal controls at the Service Center. The weaknesses within the five major areas are provided below, and specific details of the weaknesses and our respective recommendations to improve these weaknesses are in Appendix 1.

Computer Center Management and Operations

We found that contractor employees in critical positions did not have proper background clearances, Without knowledge of security-related background information on contractor personnel, the risk is increased for Service Center's sensitive systems to be compromised. We made one recommendation to address this weakness.

LAN Protection

We found that the Service Center could improve controls in administering and managing its LAN. Improved controls were needed in the areas of intruder detection lockout settings, disaster recovery, and user access. Because of the weak controls, the risk is increased for Service Center personnel to have unauthorized access to the mainframe computer and thus to sensitive payroll and accounting data. We made five recommendations to address these weaknesses.

FFS Application

We found that access controls in the FFS application software would not prevent Service Center users from generating unauthorized disbursements. Specifically, several users had access to vendor tables, which could result in the tables being changed and disbursing documents being affected. We made one recommendation to correct this weakness,

Mainframe Computer System Physical and Logical Security

We found that the Service Center did not always comply with Circular A- 130 or the Department of the Interior's "Information System Security Handbook." Also, the Service Center did not implement controls recommended in software vendor guidelines and generally accepted information system industry practices in administering and implementing operating system and access security software on its mainframe computers. These weaknesses were in the areas of physical security, password settings, System Management Facility (SMF) logs, multiple user identification (ID) codes, ADP access levels, separation of duties in the use of RACF security controls, and computer security plans. As a result, sensitive data maintained on the Service Center's computer were vulnerable to unauthorized access and change. We made 14 recommendations to address weaknesses in these areas.

Contingency Planning, Backup, and Disaster Recovery

We found weaknesses in the Service Center's contingency planning, backup, and disaster recovery for its sensitive systems and mainframe computing environment. Specifically, rather than relying on documented procedures, the Service Center relied upon individuals' knowledge. We also found that the Service Center did not have a documented comprehensive business recovery plan. As a result, in the event of a disaster, the Service Center may not be able to recover critical systems and business functions. We made three recommendations to address these weaknesses.

Bureau of Reclamation Response and Office of Inspector General Reply

In the March 24, 1997, response (Appendix 2) from the Commissioner, Bureau of Reclamation, to our draft report, the Bureau generally concurred with 23 of our 24 recommendations. Based on the response, we consider Recommendations A.1, D.1, D.2, E.1, F.1, F.2, F.3, H.1, H.2, I.2, J.2, M.1, and N.1 resolved and implemented; Recommendations B.1, C.1, D.3, G.1, G.2, I.1, J.1, K.1, N.2, and 0.1 resolved but not implemented; and Recommendation L. 1 unresolved. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation, and the Bureau is requested to reconsider the unresolved recommendation (see Appendix 3). While the Bureau's response generally concurred with the recommendations, except for Recommendation L. 1, the response did take issue with several statements regarding our recommendations, which we have addressed as follows:

- Recommendation L.1. The Bureau said that it "disagree[d]" with the recommendation and that it "question[ed] any adverse effect as well as any benefit from retroactively requiring additional documentation [to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments]. While we did not question the validity of oral requests for access to the mainframe computer systems, we did recommend that these requests and approvals be documented in Facility records to allow reconciliation between access requested and access allowed to ensure that access is assigned at the appropriate level. Accordingly, the Bureau should reconsider its response to this recommendation.

- Recommendation F.1. While the Bureau said that it has complied with the recommendation, it stated that the problem was "currency of documentation" and not a problem of physical security because two levels of security control occur before personnel are allowed entry into the computer rooms. We agree that two levels of security control had to be passed through to enter the computer room. However, the Service Center had "generic" key cards that were issued to and used by vendors and building management personnel for access to the computer rooms. Thus there was little assurance that only specific people had use of the key card to gain access to the computer rooms.

- Recommendation G.2. While the Bureau said that it concurred with the intent of the recommendation, it stated in its response that the 180-day password interval for RACF security applied to only one application, the Automated SF 52 System. The Bureau stated that the "extended interval" was requested by the users and approved by the Bureau's Security Manager. It further disagreed with our assertion that "not all mainframe applications have access security." We disagree with these statements. First, the Automated SF 52 System is not the only application residing on the mainframe. The mainframe also houses the PAY/PERS and the Federal Financial System, both sensitive applications. Further, at the time the Service Center received approval for the 180-day password interval in June 1994, the PAY/PERS was not residing on the mainframe. Second, the PAY/PERS does not have adequate security within the application; thus it relies exclusively on

RACF security to control access. As such, by default, users to the mainframe applications have 180-day password settings.

- Recommendation K.1. While the Bureau concurred with the recommendation, it disagreed that the condition was caused by the limited number of staff assigned to the group for monitoring security. The Bureau stated, "This information does not represent the ASC [Administrative Service Center] position." During our review, we found that the group did not have an adequate number of staff or that the work load was distributed to ensure that the segregation of duties was adequate.

- Recommendation N.1. While the Bureau concurred with the recommendation, it stated that "this condition should have been more appropriately stated as a currency of documentation issue" because the Administrative Service Center "has addressed recovery of the Federal Financial System and telecommunications although not formally documented." We disagree. By not including the Federal Financial System and telecommunications in the Continuity of Operations Plans, there is little assurance that the Federal Financial System and telecommunications would be addressed and recovered during the testing of the plan or in the event of a disaster. Further, during our review of a disaster recovery test, the Federal Financial System was not included in any of the tests performed by the Service Center.

Additional Comments on Audit Report

In its response, the Bureau disagreed with our use of "generally accepted industry and information system standards" as acceptable criteria, stating that "a conclusive set of standards were not available and the auditors were not aware as to whether these standards had ever been issued as official Government-wide policy." The Bureau further stated that the Department's Office of Information Resources Management had likewise advised that it was unaware of these standards and of their applicability to Departmental organizations,

However, computer and information system audit guidelines that were used by the auditors in performing the audit are those that are also used by other Federal Government and private industry auditors and computer installation staff in evaluating the effectiveness of computer center management and operations, The audit guidelines refer to numerous directives, policies, and guidelines issued by the Office of Management and Budget and the National Institute of Standards and Technology and, by reference, to non-Federal standard-setting organizations such as the Information Systems Control Foundation, the Institute of Internal Auditors Research Foundation, and the American Institute of Certified Public Accountants. Further, the Office of Management and Budget and the National Institute of Standards and Technology, by reference, include and recognize not only these non-Federal standard-setting organizations but also the British Standards Institute, as well as: (1) periodicals such as the Auerbach Publishers newsletters and articles (EDP Audit and Control Newsletter), LAN Times, and Infosecurity News; (2) symposiums and conferences held by the Institute of Electrical and Electronic Engineers Computer Society, the National Computer Security, and UNIX; and (3) individuals who are considered experts in information systems such as the Inspector General for the U.S. House of Representatives. While guidelines and standards issued by these organizations, publishers, and individuals may not have been issued as “official Governmentwide policy,” they promulgate industrywide standards and are the bases for many Governmental directives, policies, and guidelines issued that are related to information systems. In addition, many of the Federal Government policies, directives, and guidelines state that the requirements therein are “minimum” requirements, which implies that additional requirements or standards such as those defined by the information systems industry can and should be used.

The Bureau also questioned certain recommendations in terms of their consistency with Office of Management and Budget policies, in particular, with policies of Circulars A-123 and A-l 30. In this regard, the Bureau said that we did not consider cost as an “important consideration” when addressing “adequate” computer security controls.

Regarding the “costs” of our recommendations, we are not responsible for performing cost-benefit analyses of the computer controls needed for the Bureau’s automated information systems. Rather, the Bureau is responsible for conducting an adequate review of the risks and associated costs when it determines the controls needed in its computer systems, The auditors are responsible for determining whether the analyses were adequate for the circumstances. During our review, the Bureau could not provide us with any such analyses of cost versus risk.

While the Bureau stated that armed guard service was on-site at the Service Center 24 hours a day, we did not see a guard on-site during normal duty hours at any time during our audit. We agree that the security measures identified in the Bureau’s response reduce the risk of physical damage to the Facility and thus to computers. However, our audit was not limited to reviewing only the physical access to and the security of the Facility. It also included a review of physical access to computer hardware and software. As stated in our report, physical access to the computer rooms was not controlled or limited to only those personnel who required access to perform their day-to-day duties.

As required by the Departmental Manual (360 DM 5.3), please provide us with your written comments to this report by June 3, 1997. The response should provide the information requested in Appendix 3.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Bureau Administrative Service Center personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearances

Condition: Critical contractor personnel, such as the RACF administrator and software management personnel, did not have documented clearances.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish and manage personnel security policies, standards, and procedures that include requirements for screening individuals who: (1) participate in the design, development, operation, or maintenance of sensitive applications or (2) have access to sensitive data.

Cause: While Federal employees are required to have background clearances, the Service Center did not apply this requirement to contractors.

Effect: Without proper personnel screening, managers had limited knowledge of the suitability of contractor personnel, from a security standpoint, for their respective jobs. Without this assurance, the risk is increased for the Service Center's sensitive systems to be compromised.

Recommendation:

We recommend that the Director, Administrative Service Center, require all contractor employees to have the proper background clearances.

LAN PROTECTION

B. LAN Monitoring

Condition: Four file servers at the Service Center had minimal lockout settings. For example, current lockout procedures provide for only a 15-minute lockout after three or four unsuccessful log-in attempts. We believe that these lockout settings would not adequately identify unauthorized access. The NetWare operating system software supports an “intruder detection/lockout feature,” which aids in the prevention of unauthorized access to the system. The system will suspend a user account when a predefined number of unsuccessful access attempts occurs in a predetermined amount of time. The time that an account is suspended may also be defined.

Criteria: The Privacy Act of 1974 and the Computer Security Act of 1987 require implementation of minimally acceptable security practices for improving the security and privacy of sensitive information in Federal computer systems. Office of Management and Budget Circular A-l 30 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Also, the Circular requires agencies to ensure that appropriate safeguards exist in general support systems (for example, LANs and the data processing center, including the operating system and utilities). In addition, industry standards recommend a lockout period of 7 days.

Cause: Service Center officials stated that the 15-minute lockout met the Bureau of Reclamation’s LAN standards. However, the Bureau’s LAN implementation guidelines recognize that the minimum settings for intruder lockout parameters may be unacceptable to many offices. We believe, given the sensitivity of data at the Service Center, that minimum settings are unacceptable to ensure protection from unauthorized access to sensitive data.

Effect: The minimum level of security set for the LAN increases the risk that unauthorized access to the Service Center’s LAN resources will not be detected timely.

Recommendation:

We recommend that the Director, Administrative Service Center, enhance the intruder detection settings above the Bureau of Reclamation’s policy to suspend a user account, after unsuccessful access attempts, for a period of time long enough to ensure that the user will have to contact an administrator to have the user ID reset. For example, the user ID could be suspended for 24 hours after three incorrect attempts occurred in a 24-hour period.

LAN PROTECTION

C. LAN Disaster Recovery Plan

Condition: The Service Center did not have a documented disaster recovery plan for its LAN. This weakness was identified in a March 1994 Office of Inspector General audit report (No. 94-I357). The report recommended that the Service Center complete a risk analysis (the first step in developing a disaster recovery plan) on its LAN.

Criteria: Office of Management and Budget Circular A- 130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Specifically, agencies should establish a contingency plan and periodically test the capability of the plan to perform the function in the event that its automated systems fail

Cause: Because no risk analysis has been performed on the LAN, no disaster recovery plan has been developed by the Service Center.

Effect: The lack of a disaster recovery plan increases the risk that offices will not be able to resume processing on a timely basis after a disaster occurs.

Recommendation:

We recommend that the Director, Administrative Service Center, develop and periodically update a disaster recovery plan for the LAN.

LAN PROTECTION

D. User Access Control

Condition: The security settings that provide access to the file servers were not controlled. We identified weaknesses in the way user profiles had been established. In NetWare, established user profiles superseded the file server default restrictions. As such, some users had a required password change interval greater than 90 days, had concurrent multiple or unlimited connections, and were not required to use unique passwords.

In addition, the "SECURE CONSOLE" command was not used on any of the file servers we reviewed. The "SECURE CONSOLE" command is designed to prevent users from gaining access to the file server console by removing DOS from the system memory when the operating system is powered down. Also, the "SET ALLOW UNENCRYPTED PASSWORD = ON" was found on two of the file servers reviewed. This designation allows passwords to be UNENCRYPTED, thereby increasing the risk for passwords to be obtained and used by unauthorized users.

Criteria: Office of Management and Budget Circular A- 130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems, It also requires agencies to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The Circular further defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

Cause: Service Center procedures were not followed or were not in place to ensure that controls were adequate to safeguard the LANs.

Effect: The minimum security settings for the Service Center's LAN increase the risk for unauthorized access to network systems, which could result in the loss of data and in unauthorized individuals gaining access to sensitive data files through DOS by bringing down the file server.

LAN PROTECTION

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Ensure that LAN security and password features are implemented, which will require all users to change passwords every 90 days, enforce unique password use, and limit concurrent multiple or unlimited connections to one per user and grant additional connections on an as-needed basis.

2. Include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining access to the system files in DOS mode.

3. Ensure that the command "SET ALLOW UNENCRYPTED PASSWORD=ON" is not present in the AUTOEXEC.NCF file.

FFS APPLICATION

E. Access Security Controls

Condition: FFS security access controls were not adequate. We identified 15 users, who were Service Center employees, who could update and modify the application vendor table of one of the Service Center's clients, as well as initiate disbursement documents. This access could result in the vendor table being changed and in an unauthorized disbursing document being entered.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires that security controls for personnel include such controls as individual accountability, "least privileged," and separation of duties. "Least privileged" is the practice of restricting users' access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, or delete) to the minimum necessary for the users to perform their jobs. Separation of duties is the practice of dividing the steps in a critical function among different individuals.

Cause: Although the Service Center provided payment services to its client, the Service Center had not ensured that security controls in the FFS application prevented unauthorized payments. Service Center officials stated that the client was responsible for establishing the application security.

Effect: Without the applicable security access controls, the risk is increased for unauthorized payments to be disbursed.

Recommendation:

We recommend that the Director, Administrative Service Center, coordinate with the client to limit Service Center users' access to the "least privileged" in the FFS application; that is, assurance should be provided that any user authorized to enter or change the vendor table does not also have access to disbursing documents.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

F. Physical Security

Condition: Although access to the Service Center facilities was controlled, the Service Center could not identify all individuals who had card key access to the computer rooms, which house the mainframe and LAN. In addition, some Service Center visitors (for example, maintenance personnel, janitorial staff, and vendors) were not monitored when they were inside the computer room.

Criteria: The Department of the Interior Automated Information System Handbook, when addressing the control for personnel access to computer facilities, states, "Access by visitors, equipment personnel, and other individuals not directly involved with managing or operating a sensitive automated information system installation will be controlled by individual authorization." The Handbook further states that it is recognized that different procedures and restrictions will be required for various categories of visitors but that all access by other than assigned personnel will be monitored.

Cause: The Service Center's informal procedures provided for vendors, as well as for the building management company, to be issued card keys to these sensitive areas without identifying the individuals receiving the cards and without requiring formal access request forms. Also, current practices allow certain visitors to be unmonitored when they are in the sensitive areas,

Effect: The Service Center cannot specifically identify all those individuals who have access to and/or are accessing the computer rooms. Furthermore, by not monitoring all visitors, the risk is increased for the Service Center's sensitive data and resources to be stolen or destroyed.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Document procedures for the issuance of key cards and require that the procedures be instituted for vendors in addition to contractors and Federal employees.

2. Evaluate the need for individuals outside of the ADP Services Division to be issued permanent card keys because such access should be limited to those individuals performing their day-to-day duties.

3. Document procedures to ensure the Service Center's compliance with the Department of the Interior Automated Information Systems Handbook regarding visitor (such as maintenance personnel, janitorial staff, and vendors) monitoring.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

G. Password Settings

Condition: In RACF, general client user passwords for access to the mainframe were not prompted for change until after 180 days, and user ID codes were not automatically revoked until 180 days of inactivity.

Criteria: The Department of the Interior Automated Information Systems Security Handbook recommends that passwords be changed every 90 days. Also, generally accepted industry standards indicate that password change intervals should be from 60 to 90 days for users who do not have sensitive privileges and every 30 days for users who do have sensitive privileges because passwords may be guessed, copied, overheard, or recorded and played back.

Cause: To make access to the mainframe applications more convenient for Service Center clients who use the mainframe applications only occasionally, notably the SF-52 System users, the Service Center increased the password interval to 180 days in 1994 after receiving approval from the Bureau of Reclamation's Security Administrator. However, this approval recommended that the Service Center change the password parameters, such as requiring a numeric or special character as part of the password, set in RACF security software. Service Center officials stated that the 180-day interval was acceptable because of security available within the mainframe applications. However, not all of the mainframe applications have access security.

Effect: The current password settings reduce the effectiveness of the password as a control, thereby increasing the risk for unauthorized access to sensitive information through password disclosure.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate the feasibility of setting the parameters in RACF security software to require one numeric or special character as part of the password, as recommended by the Bureau of Reclamation's Security Administrator.

2. Reevaluate the standard RACF password change intervals and revocation settings to ensure that the level of risk associated with the mainframe applications and the current password settings is

acceptable to the Service Center, as well as to its clients and the Department, and address these results in a current risk assessment.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

H. SMF Logs

Condition: At least 27 Service Center user ID codes that were allowed access to the TSO software had "alter" access to the "SYS1.MAN%" dataset. The SYSl.MAN% dataset contains the SMF logs that record all system activity, thereby providing a system audit trail. In addition, a critical SMF record type, record type 60, was not active.

Criteria: Office of Management and Budget Circular A-130 recommends that adequate audit trails exist so that an adverse impact on general support systems is prevented or detected. Also, Federal Information Processing Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," provides guidelines for system security and addresses the importance of having audit trails of all system activity.

Cause: The Service Center had insufficient policies and procedures surrounding the protection of the SYS1.MAN% datasets. Also, SMF record type 60 was not active because Service Center officials said that they believed another software product INFOPAC (report generation software) created too many records. They said, therefore, that to reduce the amount of storage needed for SMF logs, record type 60 was not activated.

Effect: By allowing users "alter" access to these logs, the risk is increased for the SMF logs to be inaccurate. Furthermore, because record type 60 is not active, no system audit trail exists to determine whether the changes to sensitive datasets by authorized individuals are appropriate. Specifically, because the PAY/PERS application has no internal security to monitor access and changes to its datasets, the Service Center relies only on RACF security. The active SMF record types identified only security violations and did not record changes made to datasets. Therefore, in the PAY/PERS application, there was no system audit trail available to monitor and evaluate changes made to PAY/PERS sensitive data.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

Recommendations:

We recommend that the Director, Administrative Service Center :

1. Evaluate the feasibility of limiting the number of Service Center users who have access authority to alter SMF logs.

2. Ensure that the SMF record type 60 logging is active or RACF settings are adjusted to specifically audit critical datasets maintained on the mainframe computers and to therefore provide an audit trail of system activity.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

I. "OPERATIONS" Attribute

Condition: The Service Center gave access to all of the operating system resources by assigning the "OPERATIONS" attribute to 85 active Service Center user IDs without logging the activities of these users. Through this access, users could make unauthorized changes to the mainframe computer operating system and sensitive application datasets without being detected by routine security controls.

Criteria: The RACF Auditor's Guide states that "the OPERATIONS attribute allows a user access to almost all resources" and that the "group-OPERATIONS attribute allows a user access to almost all resources within the scope of the group and its subgroups." The "OPERATIONS" attribute, with some exceptions, provides the user with full control over datasets. Further, the RACF Security Administrator's Guide recommends that the "OPERATIONS" attribute be assigned to a minimum number of people and that the activities of the users be logged. RACF allows the use of more restrictive authorities, such as DASDVOL authority, when routine maintenance operations are performed. RACF security software also provides the option to log activities of users with the "OPERATIONS" attribute by activating the OPERAUDIT option.

Cause: The Service Center had not assigned more restrictive authorities to individuals who performed routine system maintenance tasks because the Service Center had not evaluated the system access authority needed for individual users in performing their day-to-day functions. Also, the Service Center had not implemented the OPERAUDIT security feature in RACF that would log user activities as a result of the "OPERATIONS" attribute.

Effect: Because the OPERAUDIT security feature had not been activated, any resource on the mainframe computer could be accessed using the "OPERATIONS" attribute without recording the user's access. This setting, along with the lack of system audit trails that would be produced by the SMF 60 record type, increases the risk for intentional or accidental unauthorized system actions to occur and not be detected.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate the extent to which the "OPERATIONS" attribute should be available to Service Center user IDs. Specifically, the use of other more restrictive RACF authorities (such as DASDVOL authority) should be considered where possible.

2. Activate the security feature RACF OPERAUDIT and ensure that security personnel perform periodic reviews of the resultant logs to identify unauthorized activity.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

J. ADP Access Levels

Condition: Users in the Service Center's ADP Services Division had significant access levels. For example, 28 user IDs had RACF authority to emulate the master console, even though the authority to issue operator commands through the TSO was not given to these individuals. In addition, 28 user IDs had "alter" access to the system parameter libraries (for example, the SYS1.PARMLIB) through the TSO.

Criteria: Office of Management and Budget Circular A-130 requires, at a minimum, that agency programs incorporate controls such as "separation of duties, least privileged, and individual accountability" within their major applications.

Cause: Because of other Service Center priorities, the group responsible for monitoring security had not performed an audit of user access levels and therefore had not identified the required necessary changes and had not ensured that user access was at the authorized level. In addition, the ADP Services Division had not implemented procedures to ensure that "least privileged" access controls and appropriate separation of duties were in place.

Effect: By allowing significant access levels to critical functions, the risk is increased for datasets to be altered without authorization and for the alteration to go undetected by normal operating controls. Without periodic review of user access levels, the risk is increased that the access given to a user will exceed that which is necessary to perform the user's daily job.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Ensure that the group responsible for monitoring security performs periodic reviews of user access levels to identify required necessary changes and to ensure that user access levels are authorized.

2. Institute a policy of "least privileged" access levels to ensure that access to resources and data is limited to those users who require such access.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

K. RACF Software Internal Controls

Condition: Responsibilities of the RACF security administrator (assigned the SPECIAL attribute within RACF) had been combined with the responsibilities of the RACF auditor (assigned the AUDITOR attribute within RACF). In addition, seven user IDs within the Service Center had these combined attributes. This weakness was previously identified in a March 1994 Office of Inspector General audit report (No. 94-I-357).

Criteria: The RACF Auditor's Guide addresses the importance of the separation of duties between the security administrator and the auditor. The Guide states, "The separation of powers is necessary because it is the security administrator's job to establish RACF controls, and it is the auditor's function to test the adequacy and effectiveness of these controls. "

Cause: Service Center officials stated that RACF security administrator and RACF auditor functions were performed by the same individual because of the limited number of staff assigned to the group responsible for monitoring security. They further stated that the Service Center had a limited number of individuals who had expertise in the area of RACF administration,

Effect: The control over the RACF security administrator function is lost because there was no systematic monitoring of this powerful function. Therefore, the risk exists for accidental or intentional unauthorized actions that could disrupt information system operations and threaten the integrity of the sensitive information.

Recommendation:

We recommend that the Director, Administrative Service Center, evaluate the staffing requirements of the group responsible for monitoring security to ensure the separation of duties within RACF.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

L. Authorization - Internal Controls

Condition: Mainframe access given to users as assigned in RACF was not always supported by a formal request or was not recorded in the Service Center's Decentralized Security Administration Facility.

Criteria: The Service Center's policy is for formal authorization requests to be obtained from the designated security point of contact before users are permitted to access sensitive data on the mainframe computer. In addition, the point of contact can orally notify the Service Center for adjustments to the users' access requirements. Also, generally accepted industry standards recommend that reconciliations exist between what has been formally requested and what access level was actually granted to ensure that mishandling, alterations, and misunderstandings are reduced.

Cause: Orally requested access level adjustments that were approved were not always recorded in the access request system because the Service Center did not always enforce the procedures to record approved access level adjustments.

Effect: By not updating Decentralized Security Administration Facility records for adjustments to accesses requested, the system administrator cannot reconcile the formal authorization and the Decentralized Security Administration Facility records with the RACF access levels assigned to users and thus ensure that access is assigned at the appropriate level.

Recommendation:

We recommend that the Director, Administrative Service Center, document and implement procedures to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments to allow for the reconciliation of access requested with access allowed.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

M. Computer Security Plan/Report

Condition: The Service Center had not developed a security plan for fiscal year 1996

Criteria: The Computer Security Act of 1987 requires that all agencies improve the security and privacy of sensitive information in Federal computer systems. Specifically, the Act requires that security plans be developed for all sensitive computer systems. A computer security plan is designed to assist agencies in addressing the protection of general support systems and major applications that contain sensitive information to help ensure the system's integrity, availability, and confidentiality. In addition, Office of Management and Budget Circular A-130, Appendix III, states that agencies without adequate security plans should consider classifying this as a material weakness in their annual Federal Managers' Financial Integrity Act report to the Congress.

Cause: A computer security plan was not prepared for fiscal year 1996 because of limited staffing in the group responsible for monitoring security.

Effect: Without this plan, the Service Center did not have adequate assurance that data in its sensitive systems were adequately protected. In addition, the Service Center had a material weakness, which should be reported in its annual Federal Managers' Financial Integrity Act report to the Congress.

Recommendation:

We recommend that the Director, Administrative Service Center, provide resources to ensure the development of a computer security plan for the sensitive systems in accordance with the Computer Security Act and Circular A-130, Appendix III.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

N. Continuity of Operations Plan

Condition: The Service Center's Continuity of Operations Plan (dated December 28,1995) did not address recovery of one of the sensitive systems, the FFS; the LAN; and critical telecommunications links. Also, the Plan had not been updated to reflect all tests of the Plan completed in 1996. Additionally, the risk analysis, upon which the Plan is to be based, had not been updated since July 1990.

Criteria: Office of Management and Budget Circular A- 130 requires agencies to establish a comprehensive contingency plan and periodically test the capability to perform the agency function supported by the application, as well as critical telecommunications links, in the event of a disaster or system failure. In order to accurately and successfully test the disaster recovery capabilities, the disaster recovery plans need to be updated as changes occur. In addition, the Circular states that "manual procedures are generally NOT [emphasis in original] a viable back-up option."

Cause: Service Center officials said that update of the risk analysis and continuity of operations plan had low priorities. In addition, Service Center officials stated that the FFS application was not included in the Plan as a result of Service Center clients agreeing that FFS services could be delayed for 30 days because processing could be performed manually. However, we found no documentation of such agreements.

Effect: If the Continuity of Operations Plan is incorrect (such as by not including all sensitive systems) or is outdated, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in the event of a disaster or system failure.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Perform a risk analysis of the Service Center's computer center and its applications.

2. Update the existing Continuity of Operations Plan for the mainframe, sensitive applications, and telecommunications links so that the current operating environment is documented.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

O. Comprehensive Business Recovery Plan

Condition: No comprehensive business recovery plan had been developed for the Service Center. The only plan in existence at the Service Center was the Continuity of Operations Plan, which addressed only the recovery of the systems environment. The Plan did not address business and user operations that need to be in effect for the Service Center to support its clients in the event of a disaster or system failure.

Criteria: Office of Management and Budget Circular A-l 30 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, generally accepted information systems standards recognize that a comprehensive business recovery plan is necessary to ensure the timely recovery of all business functions and of the systems environment, both of which are critical for day-to-day operations, and to minimize down time.

Cause: The Service Center's emphasis was on the restoration of the mainframe environment rather than on the recovery of business operations.

Effect: If a disaster or system failure occurs, the Service Center may not be able to recover all business functions and systems necessary for the continued long-term operations of the organization.

Recommendation:

We recommend that the Director, Administrative Service Center, develop a comprehensive business recovery plan, which includes procedures for its business functions.

United States Department of the Interior

BUREAU OF RECLAMATION
Washington. D.C. 20240

IS REPLY REFER TO

MAR 2 4 1997

D-5010
ADM-8.00

MEMORANDUM

To: Office of Inspector General
Attention: Acting Assistant Inspector General for Audits

From: Eluid L. Martinez
Commissioner

Subject: Draft Audit Report on Mainframe Computer Policies and Procedures (Assignment No. A-IN-BOR-001-96)

The Bureau of Reclamation appreciates the opportunity to comment on the subject report. Reclamation concurs or has complied with 23 of the 24 of the audit recommendations and we fully recognize the importance of computer security and that our policies and procedures can be improved. However, we believe the Administrative Service Center (ASC) has in place an adequate security program and are concerned with certain aspects of the report as outlined below.

The report identified physical security as a weakness, We believe extensive physical security measures are in place at the ASC. The computer and related hardware (such as mainframe computer, direct access storage devices, tape devices, telecommunications equipment, large volume printers, etc.) are located in a locked computer room controlled for authorized access only. In addition, the computer room is located in a secure building where all outside doors are locked and require an individual access card for authorized entry. ASC security also includes on-site armed guard service 24 hours a day, 7 days a week. Following the Oklahoma City bombing, the Justice Department was directed by the President to conduct a Vulnerability Assessment of Federal Facilities. This assessment recognized five levels of security for Federal facilities based upon perceived threat and established security standards for each of the live levels. Based on this criteria, the ASC was deemed a Level III facility. The GSA participated in a review of ASC security and concluded the ASC exceeded Level III security requirements.

The audit report identified areas to reduce security risks and recommended specific actions to reduce those risks. Both OMB Circulars A-123 and A-130 recognize cost as an important consideration and require that agencies implement cost effective management and internal controls. For instance, OMB Circular A-130 recognizes both risk and cost in addressing “adequate security.” Yet, discussions with the auditors confirmed that cost was not considered in recommending these specific actions to reduce risk.

The audit report referred to "generally accepted industry and information systems standards" and reported the ASC as noncompliant in several instances. Discussions with the auditors confirmed that a conclusive set of these "standards" was not available and the auditors were not aware as to whether these "standards" had ever been issued as official Government-wide policy. The Department of the Interior's Office of Information Resources Management likewise advised that they were unaware of these "standards" and their applicability to Interior organizations.

Again, we appreciate the opportunity to comment on the subject report. Attached are our specific comments for each recommendation. If you have any questions or require additional information, please contact Luis Maez at (303) 236-3289, extension 245.

Attachment

cc: Assistant Secretary - Water and Science, Attention: Margaret Carpenter
(w/attachment)

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearances

Condition: Critical contractor personnel, such as the RACF administrator and software management personnel, did not have documented clearances.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish and manage personnel security policies, standards, and procedures that include requirements for screening individuals who: (1) participate in the design, development, operation, or maintenance of sensitive applications or (2) have access to sensitive data.

Cause: While Federal employees are required to have background clearances, the Service Center did not apply this requirement to contractors.

Effect: Without proper personnel screening, managers had limited knowledge of the suitability of contractor personnel, from a security standpoint, for their respective jobs. Without this assurance, the risk is increased for the Service Center's sensitive systems to be compromised.

Recommendation

We recommend that the Director, Administrative Service Center, require all contractor employees to have the proper background clearances.

Response

Complied. All ADP contractor employees, including RACF administrators and systems software management personnel, are required to have background clearances. The Statement of Work for the GSA Tri-Part Contract (which ADP Services Division uses) contained a Level 3, critical-sensitive requirement, but this provision was not previously enforced. Also, at our request, the Colorado Bureau of Investigation has completed background investigations on all ADP contractor personnel. This is also a continuing requirement for all new-hire contractor personnel.

LAN PROTECTION

B. LAN Monitoring

Condition: Four file servers at the Service Center had minimal lockout settings. For example, current lockout procedures provide for only a 15-minute lockout after three or four unsuccessful log-in attempts We believe that these lockout settings would not adequately identify unauthorized access. The NetWare operating system software supports an "intruder detection/lockout feature," which aids in the prevention of unauthorized access to the system. The system will suspend a user account when a predefined number of unsuccessful access attempts occurs in a predetermined amount of time. The time that an account is suspended may also be defined.

Criteria: The Privacy Act of 1974 and the Computer Security Act of 1987 require implementation of minimally acceptable security practices for improving the security and privacy of sensitive information in Federal computer systems. Office of Management and Budget Circular A-130 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Also, the Circular requires agencies to ensure that appropriate safeguards exist in general support systems (for example, LANs and the data processing center, including the operating system and utilities). In addition, industry standards recommend a lockout period of 7 days.

Cause: Service Center officials stated that the 15-minute lockout met the Bureau of Reclamation's LAN standards. However, the Bureau's LAN implementation guidelines recognize that the minimum settings for intruder lockout parameters may be unacceptable to many offices. We believe, given the sensitivity of data at the Service Center, that minimum settings are unacceptable to ensure protection from unauthorized access to sensitive data.

Effect: The minimum level of security set for the LAN increases the risk that unauthorized access to the Service Center's LAN resources will not be detected timely.

Recommendation

We recommend that the Director, Administrative Service Center, enhance the intruder detection settings above the Bureau of Reclamation's policy to suspend a user account, after unsuccessful access attempts, for a period of time long enough to ensure that the user will have to contact an administrator to have the user ID reset. For example, the user ID could be suspended for 24 hours after three incorrect attempts occurred in a 24-hour period.

LAN PROTECTION

Response

Concur with intent. Although lockout settings already meet Reclamation LAN standards, we are willing to consider additional security enhancements as deemed appropriate. An evaluation will be made to determine if the settings should be changed. This evaluation is scheduled to be completed by June 30, 1997. The responsible official is the Chief, ADP Services Division.

LAN PROTECTION

C. LAN Disaster Recovery Plan

Condition: The Service Center did not have a documented disaster recovery plan for its LAN. This weakness was identified in a March 1994 Office of Inspector General audit report (No. 94-I357). The report recommended that the Service Center complete a risk analysis (the first step in developing a disaster recovery plan) on its LAN.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Specifically, agencies should establish a contingency plan and periodically test the capability of the plan to perform the function in the event that its automated systems fail.

Cause: Because no risk analysis has been performed on the LAN, no disaster recovery plan has been developed by the Service Center.

Effect: The lack of a disaster recovery plan increases the risk that offices will not be able to resume processing on a timely basis after a disaster occurs.

Recommendation

We recommend that the Director, Administrative Service Center, develop and periodically update a disaster recovery plan for the LAN.

Response

Concur. A risk analysis of the ASC LAN environment will be completed by September 30, 1997. The risk analysis will provide the basis for development of a LAN Disaster Recovery Plan which is targeted for completion by March 3 1, 1998. The responsible official is the Chief, ADP Services Division.

LAN PROTECTION

D. User Access Control

Condition: The security settings that provide access to the file servers were not controlled. We identified weaknesses in the way user profiles had been established. In NetWare, established user profiles superseded the file server default restrictions. As such, some users had a required password change interval greater than 90 days, had concurrent multiple or unlimited connections, and were not required to use unique passwords.

In addition, the "SECURE CONSOLE" command was not used on any of the file servers we reviewed. The "SECURE CONSOLE" command is designed to prevent users from gaining access to the file server console by removing DOS from the system memory when the operating system is powered down. Also, the "SET ALLOW UNENCRYPTED PASSWORD = ON" was found on two of the file servers reviewed. This designation allows passwords to be UNENCRYPTED, thereby increasing the risk for passwords to be obtained and used by unauthorized users.

Criteria: Office of Management and Budget Circular A- 130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. It also requires agencies to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The Circular further defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. "

Cause: Service Center procedures were not followed or were not in place to ensure that controls were adequate to safeguard the LANs.

Effect: The minimum security settings for the Service Center's LAN increase the risk for unauthorized access to network systems, which could result in the loss of data and in unauthorized individuals gaining access to sensitive data files through DOS by bringing down the file server.

LAN PROTECTION

Recommendations

We recommend that the Director, Administrative Service Center:

1. Ensure that LAN security and password features are implemented, which will require all users to change passwords every 90 days; enforce unique password use; and limit concurrent multiple or unlimited connections to one per user and grant additional connections on an as-needed basis.

Response

Complied. The password change interval has been changed to 90 days or less on all servers. Unique passwords are now required for all individual users. Concurrent multiple connection authority has been removed from all accounts with the exception of those where a demonstrated need. exists. Requests for multiple concurrent connections now require completion of an ASC-14 Computer Security Access Request Form with appropriate supervisory authorization.

2. Include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining access to the system files in DOS mode.

Response

Complied. A procedure to secure the console on all ASC file servers was implemented in August 1996. The "LOAD MONITOR" command with the "lock" option was included in the AUTOEXEC.NCF file in January 1997.

3. Ensure that the command "SET ALLOW UNENCRYPTED PASSWORD=ON" is not present in the AUTOEXEC.NCF file.

Response

Concur. The "SET ALLOW UNENCRYPTED PASSWORD=ON" command cannot be set at this time. Certain versions of the NETWARE "NETX" client requestor are present on some ASC workstations that are not compliant with the encrypted password feature. When the migration to Netware 4. lx NDS (Novell Directory Services) is completed at the ASC and all client workstations have been migrated to Netware VLMs, this command will be invoked on all file servers. Migration to NDS will be completed as part of a Reclamation-wide effort. Although unencrypted passwords are accepted at this time, the vast majority of passwords processed by ASC file servers are currently encrypted. Target date for completion is March 3 1, 1998. The responsible official is the Chief, ADP Services Division.

FFS APPLICATION

E. Access Security Controls

Condition: FFS security access controls were not adequate. We identified 15 users. who were Service Center employees. who could update and modify the application vendor table of one of the Service Center's clients, as well as initiate disbursement documents. This access could result in the vendor table being changed and in an unauthorized disbursing document being entered.

Criteria: Office of Management and Budget Circular A-l30, Appendix III, requires that security controls for personnel include such controls as individual accountability, "least privileged," and separation of duties. "Least privileged" is the practice of restricting users' access (to **data** files, to processing capability, or to peripherals) or type of access (read, write, execute, or delete) to the minimum necessary for the users to perform their jobs. Separation of duties is the practice of dividing the steps in a critical function among different individuals.

Cause: Although the Service Center provided payment services to its client, the Service Center had not ensured that security controls in the FFS application prevented unauthorized payments.

Effect: Without the applicable security access controls, the risk is increased for unauthorized payments to be disbursed.

Recommendation

We recommend that the Director, Administrative Service Center. coordinate with the client to limit Service Center users' access to the "least privileged" in the FFS application; that is, assurance should be provided that any user authorized to enter or change the vendor table does not also have access to disbursing documents.

Response

Complied. As requested by the ASC, the client has changed FFS security such that no employees have access to both the vendor tables and disbursement function. It should be noted that this condition was confined strictly to the transfer of a client's administrative payments function and related employees to the ASC in May 1996. The client is responsible for managing and controlling FFS access for this payments function. In other words, the ASC cannot initiate or change FFS access for employees performing this client's payments. Also, it should be noted that discussions with the auditors confirmed that no unauthorized disbursements were found.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

F. Physical Security

Condition: Although access to the Service Center facilities was controlled, the Service Center could not identify all individuals who had card key access to the computer rooms, which house the mainframe and LAN. In addition, some Service Center visitors (for example, maintenance personnel, janitorial staff, and vendors) were not monitored when they were inside the computer room.

Criteria: The Department of the Interior Automated Information System Handbook, when addressing the control for personnel access to computer facilities, states, "Access by visitors, equipment personnel, and other individuals not directly involved with managing or operating a sensitive automated information system installation will be controlled by individual authorization." The Handbook further states that it is recognized that different procedures and restrictions will be required for various categories of visitors but that all access by other than assigned personnel will be monitored.

Cause: The Service Center's informal procedures provided for vendors, as well as for the building management company, to be issued card keys to these sensitive areas without identifying the individuals receiving the cards and without requiring formal access request forms. Also, current practices allow certain visitors to be unmonitored when they are in the sensitive areas.

Effect: The Service Center cannot specifically identify all those individuals who have access to and/or are accessing the computer rooms. Furthermore, by not monitoring all visitors, the risk is increased for the Service Center's sensitive data and resources to be stolen or destroyed.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Document procedures for the issuance of key cards and require that the procedures be instituted for vendors in addition to contractors and Federal employees.

Response

Complied. Procedures for the issuance of card keys for vendors, contractors, and Federal employees have been documented. As evidenced by this recommendation and Recommendation 3 (below), we believe this condition should have been more

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

appropriately **stated** as a currency of documentation issue. Two levels of security control must be passed before entry into the computer room. As concluded by GSA, ASC's physical security exceeds security standards for a Level III Federal facility. Although the ASC has always had a strong physical security emphasis and program in place, it was recently enhanced with implementation of a picture identification card system that is now compatible with the Bureau of Reclamation system for Building 67 at the Denver Federal Center.

2. Evaluate the need for individuals outside of the ADP Services Division to be issued permanent card keys because such access should be limited to those individuals performing their day-to-day duties.

Response

Complied. The evaluation was completed by the ADP Services Division and the Management Services Division in February 1997. Permanent card keys are issued to just those individuals deemed appropriate.

3. Document procedures to ensure the Service Center's compliance with the Department of the Interior Automated Information Systems Handbook regarding visitor (such as maintenance personnel, janitorial staff, and vendors) monitoring.

Response

Complied. Procedures for monitoring visitor access to the computer room have been documented by the Management Services Division in compliance with the Department of the Interior's Automated Information Systems Handbook.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

G. Password Settings

Condition: In RACF, general client user passwords for access to the mainframe were not prompted for change until after 180 days, and user ID codes were not automatically revoked until 180 days of inactivity.

Criteria: The Department of the Interior Automated Information Systems Security Handbook recommends that passwords be changed every 90 days. Also. generally accepted industry standards indicate that password change intervals should be from 60 to 90 days for users who do not have sensitive privileges and every 30 days for users who do have sensitive privileges because passwords may be guessed. copied, overheard, or recorded and played back.

Cause: To make access to the mainframe applications more convenient for Service Center clients who use the mainframe applications only occasionally, notably the SF-52 System users, the Service Center increased the password interval to 180 days in 1994 after receiving approval from the Bureau of Reclamation's Security Administrator. However, this approval recommended that the Service Center change the password parameters, such as requiring a numeric or special character as part of the password, set in RACF security software. Service Center officials stated that the 180-day inrerval was acceptable because of security available within the mainframe applications. However, not all of the mainframe applications have access security.

Effect: The current password settings reduce the effectiveness of the password as a control, thereby increasing the risk for unauthorized access to sensitive information through password disclosure.

Recommendations

We recommend that the Director. Administrative Service Center:

1. Evaluate the feasibility of setting the parameters in RACF security software to require one numeric or special character as part of the password, as recommended by the Bureau of Reclamation's Security Administrator.

Response

Concur. An evaluation of using one numeric or special character as part of the ASC standard password will be completed by September 30, 1997. The responsible official is the Chief, ADP Services Division.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

2. Reevaluate the standard RACF password change intervals and revocation settmgs to ensure that the level of risk associated with the mainframe applications and the current password settings is acceptable to the Service Center, as well as to its clients and the Department, and address these results in a current risk assessment.

Response

Concur with intent. The ASC plans to reconfirm the 180-day interval with clients and the Department System Owner. This effort is targeted for completion September 30, 1997. The responsible official is the Chief, ADP Services Division.

It should be noted, however, that the 180-day password interval exists for only one application....the automated SF-52 System. The extended interval was requested by clients primarily for infrequent users of the system and was coordinated with the Department of the Interior System Owner and the Interior Department's Office of Information Resource Management. In addition a waiver to use the 1 80-day interval was obtained from the Bureau of Reclamation Computer Security Manager per the procedures set forth in 375 DM 19. It should also be noted that while 180 days is the overall system maximum, the password expiration period for each user is set individually by the client's Security Point-of-Contact based on their evaluation of the risk associated with the user. The ASC has issued guidance to its clients recommending that the expiration period of 180 days only be used for infrequent users of the system whose access presents a low risk. Finally, the last two sentences of the "Cause:" refer to mainframe applications and whether or not they have access security. Since the 180-day interval only relates to the automated SF-52 System which does have access security, the two sentences are not relevant to this issue.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

H. SMF Logs

Condition: At least 27 Service Center user ID codes that were allowed access to the TSO software had "alter" access to the "SYSl.MAN%" dataset. The SYS1.MAN% dataset contains the SMF logs that record all system activity. thereby providing a system audit trail. In addition a critical SMF record type, record type 60, was not active.

Criteria: Office of Management and Budget Circular A-130 recommends that adequate audit trails exist so that an adverse impact on general support systems is prevented or detected. Also, Federal Information Processing Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," provides guidelines for system security and addresses the importance of having audit trails of ail system activity.

Cause: The Service Center had insufficient policies and procedures surrounding the protection of the SYS1.MAN% datasets. Also, SMF record type 60 was not active because Service Center officials said that they believed another software product INFOPAC (report generation software) created too many records. They said, therefore, that to reduce the amount of storage needed for SMF logs, record type 60 was not activated.

Effect: By allowing users "alter" access to these logs, the risk is increased for the SMF logs to be inaccurate. Furthermore, because record type 60 is not active, no system audit trail exists to determine whether the changes to sensitive datasets by authorized individuals are appropriate. Specifically, because the PAY/PERS application has no internal security to monitor access and 'changes to its datasets, the Service Ctnter relies only on RACF security. The active SMF record types identified only security violations **and** did not record changes made **to datasets.** Therefore. in the PAY/PERS application, there was no system audit trail available to monitor and evaluate changes made to PAY/PERS sensitive **data.**

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY __

Recommendations

We recommend that the Director. Administrative Service Center :

1. Evaluate the feasibility of limiting the number of Service Center users who have access authority to alter SMF logs.

Response

Complied. The evaluation was completed in December 1996 to limit the number of individuals with access authority to alter SAF logs. This authority has now been limited to just three senior level system programmers that reside in the System Software Management Branch. The evaluation was completed by the Chief, Systems Management Branch, the ASC Computer Security Manager and approved by the Chief, ADP Services Division.

2. Ensure that the SMF record type 60 logging is active or RACF settings are adjusted to specifically audit critical datasets maintained on the mainframe computers and to therefore provide an audit trail of system activity.

Response

Complied. Batch and TSO type 60 records have always been written to the SMF log. Type 60 record collection has now been activated for “started tasks” as well.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

I. "OPERATIONS" Attribute

Condition: The Service Center gave access to all of the operating system resources by assigning the "OPERATIONS" attribute to 85 active Service Center user IDs without logging the activities of these users. Through this access, users could make unauthorized changes to the mainframe computer operating system and sensitive application datasets without being detected by routine security controls.

Criteria: The RACF Auditor's Guide states that "the OPERATIONS attribute allows a user access to almost all resources" and that the "group-OPERATIONS attribute allows a user access to almost all resources within the scope of the group and its subgroups." The "OPERATIONS" attribute, with some exceptions, provides the user with full control over datasets. Further. the RACF Security Administrator's Guide recommends that the "OPERATIONS" attribute be assigned to a minimum number of people and that the activities of the users be logged. RACF allows the use of more restrictive authorities, such as DASDVOL authority, when routine maintenance operations are performed. RACF security software also provides the option to log activities of users with the "OPERATIONS" attribute by activating the OPERAUDIT option.

Cause:, The Service Center had not assigned more restrictive authorities to individuals who performed routine system maintenance tasks because the Service Center had not evaluated the system access authority needed for individual users in performing their day-to-day functions. Also, the Service Center had not implemented the OPERAUDIT security feature in RACF that would log user activities as a result of the "OPERATIONS" attribute.

Effect: Because the OPERAUDIT security feature had not been activated, any resource on the mainframe computer could be accessed using the "OPERATIONS" attribute without recording the user's access. This setting, along with the lack of system audit trails that would be produced by the SMF 60 record type, increases the risk for intentional or accidental unauthorized system actions to occur and not be detected.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

Recommendations

We recommend that the Director, Administrative Service Center:

1. Evaluate the extent to which the "OPERATIONS" attribute should be available to Service Center user IDs. Specifically, the use of other more restrictive RACF authorities (such as DASDVOL authority) should be considered where possible.

Response

Concur. An evaluation will be conducted to limit the "OPERATIONS" attribute to those authorized ADP personnel deemed necessary and appropriate as well as consider other more restrictive RACF authorities. Target date for completion is December 31, 1997. The responsible official is the Chief, ADP Services Division.

2. Activate the security feature RACF OPERAUDIT and ensure that security personnel perform periodic reviews of the resultant logs to identify unauthorized activity.

Response

Complied. The feature RACF OPERAUDIT has been activated and the resultantlogs will be reviewed on a quarterly basis by the ASC Computer Security Manager. It should be noted that this situation is restricted to ADP authorized personnel only.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

J. ADP Access Levels

Condition: Users in the Service Center's ADP Services Division had significant access levels. For example, 28 user IDs had RACF authority to emulate the master console, even though the authority to issue operator commands through the TSO was not given to these individuals. In addition 28 user IDs had "alter" access to the system parameter libraries (for example, the SYS1.PARMLIB) through the TSO.

Criteria: Office of Management and Budget Circular A-130 requires, at a minimum, that agency programs incorporate controls such as "separation of duties, least privileged, and individual accountability" within their major applications.

Cause: Because of other Service Center priorities. the group responsible for monitoring security had not performed an audit of user access levels and therefore had not identified the required necessary changes and had not ensured that user access was at the authorized level. In addition, the ADP Services Division had not implemented procedures to ensure that "least privileged" access controls and appropriate separation of duties were in place.

Effect: By allowing significant access levels to critical functions, the risk is increased for datasets to be altered without authorization and for the alteration to go undetected by normal operating controls. Without periodic review of user access levels, the risk is increased that the access given to a user will exceed that which is necessary to perform the user's daily job.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Ensure that the group responsible for monitoring security performs periodic reviews of user access levels to identify required necessary changes and to ensure that user access levels are authorized.

Response

Concur. A project to identify and initialize auditing for all critical sensitive datasets will be started. The target date for completion is June 30, 1997. The responsible official is Chief, ADP Services Division.

MAINFRAME SYSTEM PHYSICAL AND LOGICAL SECURITY

2. Institute a policy of "least privileged" access levels to ensure that access to resources and data is limited to those users who require such access.

Response

Complied. A policy of "least privileged" access is now in place. While the capability to emulate the master console is assigned to a few individuals, the ability to issue critical operating system level commands has not been given. These commands are limited to the master console which is located in a locked, secured computer room accessible by authorized personnel only.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

K. RACF Software Internal Controls

Condition: Responsibilities of the RACF security administrator (assigned the SPECIAL attribute within RACF) had been combined with the responsibilities of the RACF auditor (assigned the AUDITOR attribute within RACF). In addition, seven user IDs within the Service Center had these combined attributes. This weakness was previously identified in a March 1994 Office of Inspector General audit report (No. 94-I-357).

Criteria: The RACF Auditor's Guide addresses the importance of the separation of duties between the security administrator and the auditor. The Guide states, "The separation of powers is necessary because it is the security administrator's job to establish RACF controls, and it is the auditor's function to test the adequacy and effectiveness of these controls. "

Cause: Service Center officials stated that RACF security administrator and RACE-auditor functions were performed by the same individual because of the limited number of staff assigned to the group responsible for monitoring security. They further stated that the Service Center had a limited number of individuals who had expertise in the area of RACF administration.

Effect: The control over the RACF security administrator function is lost because there was no systematic monitoring of this powerful function. Therefore, the risk exists for accidental or intentional unauthorized actions that could disrupt information system operations and threaten the integrity of the sensitive information.

Recommendation

We recommend that the Director, Administrative Service Center, evaluate the staffing requirements of the group responsible for monitoring security to ensure the separation of duties within RACF.

Response

Concur. Staffing requirements will be evaluated to ensure the separation of duties within RACF. Separation of RACF administrator and auditor responsibilities will be accomplished to the maximum extent possible. However, combining these responsibilities in isolated situations is necessary and will be managed accordingly. Also, we disagree with the statement that this condition was caused by "the limited number of staff assigned to the group responsible for monitoring security." This information does not represent the ASC position. The target date for completion of this evaluation is September 30, 1997. The responsible official is the Chief, ADP Services Division.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

L. Authorization - Internal Controls

Condition: Mainframe access given to users as assigned in RACF was not always supported by a formal request or was not recorded in the Service Center's Decentralized Security Administration Facility.

Criteria: The Service Center's policy is for formal authorization requests to be obtained from the designated security point of contact before users are permitted to access sensitive data on the mainframe computer. In addition, the point of contact can orally notify the Service Center for adjustments to the users' access requirements. Also, generally accepted industry standards recommend that reconciliations exist between what has been formally requested and what access level was actually granted to ensure that mishandling, alterations, and misunderstandings are reduced.

Cause: Orally requested access level adjustments that were approved were not always recorded in the access request system because the Service Center did not always enforce the procedures to record approved access level adjustments.

Effect: By not updating Decentralized Security Administration Facility records for adjustments to accesses requested, the system administrator cannot reconcile the formal authorization and the Decentralized Security Administration Facility records with the RACF access levels assigned to users and thus ensure that access is assigned at the appropriate level.

Recommendation

We recommend that the Director, Administrative Service Center, document and implement procedures to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments to allow for the reconciliation of access requested with access allowed.

Response

Nonconcur. We disagree there is a problem and question any adverse effect. Formal requests for user access are made through client Security Points-of-Contact to the ASC Security Manager. As users begin accessing the system revisions to their access are sometimes necessary in order to perform their duties. To expedite these revisions, client Security Points-of-Contact may orally contact the ASC Security Manager. Since only client and ASC security officials can effect these access revisions, we question any adverse effect as well as any benefit from retroactively requiring additional documentation. Also, “generally accepted industry standards” are cited as applicable criteria. As previously addressed in our response, discussions with the auditors confirmed that a conclusive set of “generally accepted industry and information system standards” were not available and the auditors were not aware as to whether these “standards” had ever been issued as official Government-wide policy. The Department of the Interior’s Office of Information Resources Management likewise advised that they were unaware of these “standards” and their applicability to Interior organizations. Finally, we question the recommendation in terms of consistency with OMB policies. Both OMB Circulars A-123 and A-130 recognize cost as an important consideration and require that agencies implement cost effective management and internal controls. For instance, OMB Circular A-130 recognizes both risk and cost in addressing “adequate security.” Yet, discussions with the auditors confirmed that cost was not considered.

MAINFRAME COMPUTER PHYSICAL AND LOGICAL SECURITY

M. Computer Security Plan/Report

Condition: The Service Center had not developed a security plan for fiscal year 1996.

Criteria: The Computer Security Act of 1987 requires that all agencies improve the security and privacy of sensitive information in Federal computer systems. Specifically, the Act requires that security plans be developed for all sensitive computer systems. A computer security plan is designed to assist agencies in addressing the protection of general support systems and major applications that contain sensitive information to help ensure the system's integrity, availability, and confidentiality. In addition Office of Management and Budget Circular A-130, Appendix III, states that agencies without adequate security plans should consider classifying this as a material weakness in their annual Federal Managers' Financial Integrity Act report to the Congress"

Cause: A computer security plan was not prepared for fiscal year 1996 because of limited staffing in the group responsible for monitoring security.

Effect: Without this plan the Service Center did not have adequate assurance that data in its sensitive systems were adequately protected. In addition, the Service Center had a material weakness, which should be reported in its annual Federal Managers' Financial Integrity Act report to the Congress.

Recommendation

We recommend that the Director. Administrative Service Center, provide resources to ensure the development of a computer security plan for the sensitive systems in accordance with the Computer Security Act and Circuiar A-130, Appendix III. Also, the lack of a security plan should be reported as a material weakness to the Department of the Interior for inclusion in its next annual Federal Managers' Financial Integrity Act report until a plan is developed and meets the requirements of Circular A- 130.

Response

Complied. A current computer security plan was documented and submitted in January 1997 in accordance with Department of the Interior Office of Information Resources Management requirements. The ASC has had an effective security program in place that has included, for example, periodic reviews of security controls in each major system as required by OMB Circular A-130. These reviews have disclosed no significant security problems or deficiencies.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

N. Continuity of Operations Plan

Condition: The Service Center's Continuity of Operations Plan (dated December 28,1995) did not address recovery of one of the sensitive systems, the FFS; the LAN; and critical telecommunications links. Also, the Plan had not been updated to reflect all tests of the Plan completed in 1996. Additionally, the risk analysis, upon which the Plan is to be based, had not been updated since July 1990.

Criteria: Office of Management and Budget Circular A-130 requires agencies to establish a comprehensive contingency plan and periodically test the capability to perform the agency function supported by the application, as well as critical telecommunications links, in the event of a disaster or system failure. In order to accurately and successfully test the disaster recovery capabilities, the disaster recovery plans need to be updated as changes occur. In addition the Circular states that "manual procedures are generally NOT [emphasis in original] a viable back-up option."

Cause: Service Center officials said that update of the risk analysis and continuity of operations plan had low priorities. In addition, Service Center officials stated that the FFS application was not included in the Plan as a result of Service Center clients agreeing that FFS services could be delayed for 30 days because processing could be performed manually. However, we found no documentation of such agreements.

Effect: If the Continuity of Operations Plan is incorrect (such as by not including all sensitive systems) or is outdated, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in the event of a disaster or system failure.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Perform a risk analysis of the Service Center's computer center and its applications.

Response

Complied. A risk analysis of the computer center was completed in November 1996. The security plan calls for periodic reviews of security controls for major systems in accordance with the requirements of OMB Circular A-130.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

2. Update the existing Continuity of Operations Plan for the mainframe, sensitive applications, and telecommunications links so that the current operating environment is documented.

Response

Concur. The Continuity of Operations Plan will be updated for the mainframe, sensitive applications and telecommunication links by September 30, 1997. The responsible official is the Chief, ADP Services Division. It should be noted that we believe this condition should have been more appropriately stated as a currency of documentation issue. The ASC has addressed recovery of the Federal Financial System and telecommunications although not formally documented. This will now be documented as part of the update of the Continuity of Operations Plan.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

O. Comprehensive Business Recovery Plan

Condition: No comprehensive business recovery plan had been developed for the Service Center. The only plan in existence at the Service Center was the Continuity of Operations Plan, which addressed only the recovery of the systems environment. The Plan did not address business and user operations that need to be in effect for the Service Center to support its clients in the event of a disaster or system failure.

Criteria: Office of Management and Budget Circular A-130 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, generally accepted information systems standards recognize that a comprehensive business recovery plan is necessary to ensure the timely recovery of all business functions and of the systems environment, both of which are critical for day-to-day operations, and to minimize down time.

Cause: The Service Center's emphasis was on the restoration of the mainframe environment rather than on the recovery of business operations.

Effect: If a disaster or system failure occurs, the Service Center may not be able to recover all business functions and systems necessary for the continued long-term operations of the organization.

Recommendation

We recommend that the Director, Administrative Service Center, develop a comprehensive business recovery plan, which includes procedures for its business functions.

Response

Concur with intent. Although, we are not aware of any specific requirement for a "comprehensive business recovery plan," we are willing to evaluate major operations and business functions to ensure long-term sustainability. Completion of the evaluation is targeted for March 31, 1998. The responsible official is the Chief, Management Services Division.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.1, D.1, D.2, E.1, F.1, F.2, F.3, H.1, H.2, I.2, J.2, M.1, and N.1	Implemented.	No further action is required
B.1, C.1, D.3, G.1, G.2, I.1, J.1, K.1, N.2, and O.1	Resolved: not implemented.	No further response to the Department of the Interior Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
L.1	Unresolved.	Reconsider the recommendation, and provide an action plan that includes target dates and titles of officials responsible for implementation.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior
Office of Inspector General
1849 C Street, N.W.
Mail Stop 5341
Washington, D.C. 20240

Our 24-hour
Telephone HOTLINE
1-800-424-5081 or
(202) 208-5300

TDD for hearing impaired
(202) 208-2420 or
1-800-354-0996

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior
Office of Inspector General
Eastern Division - Investigations
1550 Wilson Boulevard
Suite 410
Arlington, Virginia 22209

(703) 235-9221

North Pacific Region

U.S. Department of the Interior
Office of Inspector General
North Pacific Region
238 Archbishop F.C. Flores Street
Suite 807, PDN Building
Agana, Guam 96910

(700) 550-7428 or
COMM 9-011-671-472-7279

Toll Free Numbers:
1-800-424-5081
TDD 1-800-354-0996

FTS/Commercial Numbers:
(202) 208-5300
TDD (202) 208-2420

HOTLINE

1849 C Street, N.W.
Mail Stop 5341
Washington, D.C. 20240